中国科学 : 信息科学 2025 年 第 55 卷 第 6 期: 1534–1547
SCIENTIA SINICA Informationis
论文

基于圆上双向量子游走的多方身份认证量子密钥协商

王政, 王锦涛, 李霞, 叶天语*

浙江工商大学信息与电子工程学院, 杭州 310018
* 通信作者. E-mail: yetianyu@zjgsu.edu.cn

收稿日期: 2025–01–17; 修回日期: 2025–03–21; 接受日期: 2025–04–23; 网络出版日期: 2025–06–05

国家自然科学基金 (批准号: 62071430) 和浙江省属高校基本科研业务费专项 (批准号: JRK21002) 资助项目

摘要 本文提出一种新颖的基于圆上双向量子游走的多方认证量子密钥协商协议, 使得 N 个用户经过相互身份认证后在一个半忠诚第三方的协助下能平等地协商出最终的共享密钥. 在该协议中, 用户利用双向演化算子对初始量子游走态进行加密并通过诱骗粒子对其他用户进行身份认证, 然后其他用户利用全局移动算子对收到的量子态编码自己的私钥. 理论上的输出正确性分析和 IBM Qiskit 量子云平台上进行的量子线路仿真都证实了该协议的输出正确性. 该协议仅采用两粒子乘积态而非量子纠缠态作为初始量子资源, 且仅需要酉操作和单粒子测量. 该协议被证实具备信息论安全性, 能抵抗 Eve 发起的外在攻击, 且能抵抗 $N-1$ 个不忠诚用户发起的共谋攻击.

关键词 量子密钥协商, 量子身份认证, 圆上双向量子游走

1 前言

Bennett 和 Brassard [1] 首次提出量子密钥分配 (quantum key distribution, QKD) 的概念, 开创了量子密码学这一全新领域. 在 2004 年, Zhou 等 [2] 利用量子隐形传态首次提出量子密钥协商 (quantum key agreement, QKA) 的概念. QKA 与 QKD 的主要区别在于: QKA 要求所有用户共同平等协商生成共享密钥, 而 QKD 通过发送方分发量子态并与接收方协作验证从而最终生成共享密钥. 在 QKD 中, 发送方负责初始量子态的分发, 但密钥生成需依赖于双方的后处理 (如测量基比对等) , 而并非单方生成. QKA 的核心则是更强调所有用户的协商平等性, 避免由任何一方主导密钥生成过程.

根据参与用户的数量进行划分, QKA 可被分为两方 QKA 和多方 QKA 两类. 在 2004 年, Hsueh 和 Chen [3] 设计了一个基于最大纠缠态的 QKA 协议. 在 2009 年, Tsai 和 Hwang [4] 发现文献 [2] 协议的一个关键不足之处, 即任意用户可单独决定共享密钥. 在 2013 年, Shi 和 Zhong [5] 利用 Bell 态和纠缠交换构造了首个多方 QKA 协议; Liu 等 [6] 设计了一种基于单粒子的多方 QKA 协议; Sun 等 [7] 改进了文献 [6] 协议的效率和用户私钥隐秘性. 在 2014 年, Xu 等 [8] 提出了一个新颖的基于 GHZ 态的

引用格式: 王政, 王锦涛, 李霞, 等. 基于圆上双向量子游走的多方身份认证量子密钥协商. 中国科学: 信息科学, 2025, 55: 1534–1547, doi: 10.1360/SSI-2025-0027
Wang Z, Wang J T, Li X, et al. Multiparty quantum key agreement with identity authentication based on two-direction quantum walks on a circle. Sci Sin Inform, 2025, 55: 1534–1547, doi: 10.1360/SSI-2025-0027

多方 QKA 协议. 在 2016 年, Sun 等 [9] 设计了一种高效的基于团簇态的多方 QKA 协议. 在 2017 年, Gu 和 Hwang [10] 提出了一种改进方案来克服文献 [8] 协议的弱点. 在 2019 年, Yin 和 Ma [11] 提出了一种基于三粒子纠缠态的多方 QKA 协议; Liu 等 [12] 构造了一种基于 Bell 态和单粒子的多方 QKA 协议. 在 2020 年, Tang 等 [13] 用两种不同策略改进了文献 [12] 协议的安全性和公平性. 在 2021 年, Tang 等 [14] 基于四量子比特逻辑 Bell 态提出了两个抗集体噪声的多方 QKA 协议. 在 2022 年, Gao 和 Zhou [15] 基于类 GHZ 态和 χ^+ 态的纠缠交换提出了一个新颖的多方 QKA 协议. 在 2024 年, Yang 等 [16] 提出一种基于 N 粒子最大纠缠态的多方 QKA 协议.

在实际应用中, 存在外部攻击者冒充内部用户执行协议的情况, 因此在设计 QKA 协议时需要考虑身份认证问题. 身份认证 QKA 是量子身份认证 (quantum identity authentication, QIA) [17] 和 QKA 相结合的产物. 就我们所知, 目前仅存在文献 [18~26] 这几个身份认证 QKA 协议. 具体而言, Zhu 等 [18] 在 2021 年提出一种基于类 GHZ 态的三方相互身份认证 QKA 协议; Wu 等 [19] 在 2021 年提出基于 Bell 态纠缠交换的三方和多方身份认证 QKA 协议; He 等 [20] 在 2022 年提出基于 Bell 态纠缠交换的两方相互身份认证 QKA 协议; Xu 等 [21] 在 2022 年提出一种新颖的基于 GHZ 态的三方相互身份认证 QKA 协议; Gao 等 [22] 在 2022 年提出一种适用于光环量子通信网络的多方身份认证 QKA 协议; Li 等 [23] 在 2023 年提出一种基于单粒子和 GHZ 态的测量设备无关的多方身份认证 QKA 协议; Guo 等 [24] 在 2023 年提出一种基于六粒子纠缠态的无半可信第三方的两方身份认证 QKA 协议; Wang 等 [25] 在 2024 年提出一种基于单粒子和 Bell 态的密钥可循环使用的两方相互身份认证 QKA 协议; Zhang 等 [26] 在 2024 年提出一种基于四粒子团簇态纠缠交换的多方身份认证 QKA 协议.

然而, 不难发现, 文献 [18~21,23~26] 的协议都还存在一些不足之处. 具体而言, 文献 [18~21,23~26] 的协议都使用了比单粒子态更难制备的量子纠缠态作为量子资源; 文献 [19,20,23~26] 的协议都需要进行比单粒子测量更为复杂的量子纠缠态测量; 文献 [19,20,23,24,26] 的协议都需要进行复杂的量子纠缠交换.

如何验证用户身份的真实性是 QKA 实际应用的一个关键问题, 但之前的许多 QKA 协议忽略了这一问题, 从而对假冒攻击未必是安全的. 本文致力于将 QIA 应用到多方 QKA 来设计具有更强身份认证可靠性的多方 QKA 协议. 受文献 [27,28] 的基于量子游走的量子隐私比较协议和文献 [29] 的基于量子游走的量子安全多方求和协议的启发, 本文提出了一种新颖的基于圆上双向量子游走的多方认证 QKA 协议, 使得 N 个用户经过相互身份认证后在一个半忠诚第三方的协助下能平等地协商出最终的共享密钥. 本文协议被证实具备信息论安全性, 能抵抗 Eve 发起的外在攻击, 且能抵抗 $N-1$ 个不忠诚用户发起的共谋攻击. 本文协议具有如下优点: (1) 采用两粒子乘积态而非量子纠缠态作为初始量子资源; (2) 仅需要双向演化算子和全局移动算子, 但不需要量子纠缠交换操作; (3) 仅需要进行单粒子测量.

2　圆上双向量子游走

当游走粒子的路径构成一个圆时, 这种量子游走系统则被称为圆上量子游走系统. 令 $|p\rangle$ 和 $|c\rangle$ 分别为圆上量子游走系统的游走粒子量子态和硬币粒子量子态, $|\psi\rangle = |p\rangle \otimes |c\rangle$ 则是圆上量子游走系统的量子游走态, 其中 $p \in \{0,1,\ldots,d-1\}$, $c \in \{0,1\}$ 以及 $d = 2^l$. 令 $\mathcal{H}_p$ 和 $\mathcal{H}_c$ 分别表示圆上量子游走系统游走粒子张成的希尔伯特 (Hilbert) 空间和硬币粒子张成的希尔伯特空间, $\mathcal{H} = \mathcal{H}_p \otimes \mathcal{H}_c$ 则为圆上量子游走系统量子游走态张成的希尔伯特空间. 令 I_p 表示 $\mathcal{H}_p$ 的单位矩阵, $R_c(\omega,\theta,\zeta)$ 表示 $\mathcal{H}_c$ 的硬币算子, S 表示双向移动算子, 那么

$$U = S \cdot (I_p \otimes R_c(\omega,\theta,\zeta)) \tag{1}$$

为圆上双向量子游走系统量子游走态的双向演化算子, 其中

$$S=\sum_{a=0}^{d-1}\left[\left|(a+1) \bmod d\right\rangle\langle a|\otimes|0\rangle\langle 0|+\left|(a-1) \bmod d\right\rangle\langle a|\otimes|1\rangle\langle 1|\right], \tag{2}$$

$$R_c(\omega,\theta,\zeta)=\begin{pmatrix}\mathrm{e}^{\mathrm{i}\omega}\cos\theta & \mathrm{e}^{\mathrm{i}\zeta}\sin\theta\\ \mathrm{e}^{-\mathrm{i}\zeta}\sin\theta & -\mathrm{e}^{-\mathrm{i}\omega}\cos\theta\end{pmatrix}, \tag{3}$$

mod 为求模运算. U 的逆算子被定义为

$$U^{-1}=[S\cdot(I_p\otimes R_c(\omega,\theta,\zeta))]^{-1}=(I_p\otimes R_c(\omega,\theta,\zeta))^{-1}S^{-1}, \tag{4}$$

其中 S^{-1} 为 S 的逆算子, 被定义为

$$S^{-1}=\sum_{a=0}^{d-1}\left[\left|(a-1) \bmod d\right\rangle\langle a|\otimes|0\rangle\langle 0|+\left|(a+1) \bmod d\right\rangle\langle a|\otimes|1\rangle\langle 1|\right]. \tag{5}$$

定义 T_k 算子为

$$T_k=\sum_{a=0}^{d-1}\left|(a+k) \bmod d\right\rangle\langle a|, \tag{6}$$

其中 $k\in\mathbb{Z}$, $\mathbb{Z}$ 为整数集合, 那么式 (2) 的 S 可被表示为

$$S=T_1|0\rangle\langle 0|+T_{-1}|1\rangle\langle 1|, \tag{7}$$

式 (5) 的 S^{-1} 可被表示为

$$S=T_{-1}|0\rangle\langle 0|+T_1|1\rangle\langle 1|. \tag{8}$$

3　基于圆上双向量子游走的多方认证 QKA 协议

一个安全的 QKA 协议应遵循以下标准 [7]. (1) 正确性: 在协议结束时, 所有用户都拥有正确的最终隐秘密钥. (2) 安全性: 外在窃听者无法在不被检测到的情况下得到最终隐秘密钥. (3) 公平性: 每个用户对最终隐秘密钥的产生施加同等程度的影响, 共享隐秘密钥不能由所有用户的任何非零子集单独决定. (4) 每个用户仅能得到最终隐秘密钥, 无法得到其他用户的私钥.

假设 N 个用户, $P_1,P_2,\ldots,P_N$, 想在第三方 P_0 的帮助下协商密钥, 其中 P_0 被假定为半忠诚的, 即他会发起各种可能的攻击去试图获取 $P_1,P_2,\ldots,P_N$ 的秘密信息, 但不被允许与任何人串通 [24]. $P_1,P_2,\ldots,P_N$ 的身份密钥分别为 $\mathrm{ID}_1,\mathrm{ID}_2,\ldots,\mathrm{ID}_N$, 且他们知道彼此的身份密钥. 这里, $\mathrm{ID}_1,\mathrm{ID}_2,\ldots,\mathrm{ID}_N$ 的长度都为 n 比特. 本文提出的基于圆上双向量子游走的多方认证 QKA 协议致力于实现这一目标, 其详细过程被描述如下.

步骤 1. 用户 P_i 首先生成长度为 n 的随机整数序列 $\mathcal{O}_i$ 作为自己的私钥, 然后再生成长度为 n 的随机整数序列 $\mathcal{M}_i$, 其中 $\mathcal{O}_i=(O_{i,1},O_{i,2},\ldots,O_{i,n})$, $\mathcal{M}_i=(M_{i,1},M_{i,2},\ldots,M_{i,n})$, $O_{i,j},M_{i,j}\in\{0,1,\ldots,d-1\}$, $i=1,2,\ldots,N$, $j=1,2,\ldots,n$. 然后, P_i 计算 $X_{i,j}=O_{i,j}\oplus M_{i,j}$ 及 $h(\mathcal{X}_i)$, 并向其他用户公布 $h(\mathcal{X}_i)$, 其中 $\mathcal{X}_i=(X_{i,1},X_{i,2},\ldots,X_{i,n})$, $h(\cdot)$ 是一个单向哈希函数, $\oplus$ 为模 d 和运算, $i=1,2,\ldots,N$, $j=1,2,\ldots,n$.

步骤 2. P_i 制备量子游走态序列 $\Psi_i=(|\psi_{i,1}\rangle,|\psi_{i,2}\rangle,\ldots,|\psi_{i,n}\rangle)$, 其中 $|\psi_{i,j}\rangle=|p_{i,j}\rangle\otimes|c_{i,j}\rangle$, $p_{i,j}\in\{0,1,\ldots,d-1\}$, $c_{i,j}\in\{0,1\}$, $i=1,2,\ldots,N$, $j=1,2,\ldots,n$. 然后, P_i 对 Ψ_i 的第 j 个量子游走态 $|\psi_{i,j}\rangle$ 施加 b_j 次 $U_m=S\cdot(I_p\otimes R_c(0,\theta_m,0))$ 以产生新量子态

$$|Q_{i,j}\rangle=U_m^{b_j}|\psi_{i,j}\rangle=U_m^{b_j}(|p_{i,j}\rangle\otimes|c_{i,j}\rangle)$$

$$= \left[S \cdot \left(I_p \otimes R_c\left(0, \theta_m, 0\right)\right)\right]^{b_j} \left(\left|p_{i,j}\right\rangle \otimes \left|c_{i,j}\right\rangle\right), \tag{9}$$

其中 $\theta_m = \frac{2\pi m}{V}$, $m \in \{0, 1, \ldots, V\}$, $V \in \mathbb{Z}^+$, $b_j \in \mathbb{Z}^+$, $\mathbb{Z}^+$ 为正整数集合, $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, n$. 这样, P_i 就拥有量子态序列 $\mathcal{Q}_i = \left(\left|Q_{i,1}\right\rangle, \left|Q_{i,2}\right\rangle, \ldots, \left|Q_{i,n}\right\rangle\right)$. P_i 再用同样的方法产生 $N-2$ 个也处于 $\mathcal{Q}_i$ 的量子态序列, 因此 P_i 手中共有 $N-1$ 个均处于 $\mathcal{Q}_i$ 的量子态序列, 其中 $i = 1, 2, \ldots, N$.

步骤 3. 为了进行身份认证, P_i 生成 $N-1$ 个长度均为 n 的随机处于 $\{\left|0\right\rangle, \left|1\right\rangle, \left|+\right\rangle, \left|-\right\rangle\}$ 的诱骗粒子序列, 并将它们分别插入自己手中的 $N-1$ 个均处于 $\mathcal{Q}_i$ 的量子态序列, 其中 $\left|\pm\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle \pm \left|1\right\rangle\right)$, $i = 1, 2, \ldots N$. 具体而言, P_i 根据 ID_e 将一个诱骗粒子序列插入 $\mathcal{Q}_i$ 中以形成新序列 $\mathcal{Q}_i'$, 其插入规则为: 如果 ID_e 的第 j 个比特为 0, 那么 P_i 把诱骗粒子序列的第 j 个粒子放在 $\mathcal{Q}_i$ 的第 j 个量子态后面; 如果 ID_e 的第 j 个比特为 1, 那么 P_i 把诱骗粒子序列的第 j 个粒子放在 $\mathcal{Q}_i$ 的第 j 个量子态前面. 于是, P_i 手中共有 $N-1$ 个添加了用于身份认证的诱骗粒子的处于 $\mathcal{Q}_i'$ 的量子态序列. 这里, $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, n$, $e = 1, 2, \ldots, N$, 且 $e \neq i$.

步骤 4. 为了进行窃听检测, P_i 制备 $N-1$ 个足够长的随机处于 $\{\left|0\right\rangle, \left|1\right\rangle, \left|+\right\rangle, \left|-\right\rangle\}$ 的诱骗粒子序列, 并将它们分别随机插入 $N-1$ 个处于 $\mathcal{Q}_i'$ 的量子态序列, 从而形成 $N-1$ 个处于 $\mathcal{Q}_i''$ 的新量子态序列, 其中 $i = 1, 2, \ldots, N$. P_i 将 $N-1$ 个处于 $\mathcal{Q}_i''$ 的新量子态序列分别发送给其他 $N-1$ 个用户, 其中 $i = 1, 2, \ldots, N$.

步骤 5. P_e 收到 P_i 发送过来的处于 $\mathcal{Q}_i''$ 的量子态序列后与 P_i 一起进行窃听检测: P_i 公布 $\mathcal{Q}_i''$ 中用于窃听检测的诱骗粒子的位置和制备基; P_e 用相应的测量基测量这些诱骗粒子并将测量结果告知 P_i; P_i 分析错误率是否合理. 如果错误率高得不合理, P_i 将认为存在窃听并终止协议; 否则, 协议将被执行下一步. 这里, $i = 1, 2, \ldots, N$, $e = 1, 2, \ldots, N$, 且 $e \neq i$.

步骤 6. 在 P_e 和 P_i 执行完步骤 5 的窃听检测后, $\mathcal{Q}_i''$ 被恢复成 $\mathcal{Q}_i'$. P_i 告知 P_e $\mathcal{Q}_i'$ 中用于身份认证的诱骗粒子的测量基但不告诉它们的具体位置. P_e 根据 ID_e 将相应位置的用于身份认证的诱骗粒子提取出来并使用 P_i 告知的测量基对它们进行测量, 然后将测量结果告知 P_i. P_i 根据 P_e 公布的测量结果来计算错误率. 如果错误率合理, P_i 将认为身份认证成功; 否则, P_i 将认为身份认证失败. 这里, $i = 1, 2, \ldots, N$, $e = 1, 2, \ldots, N$, 且 $e \neq i$.

步骤 7. 在 P_e 和 P_i 执行完步骤 6 的身份认证后, $\mathcal{Q}_i'$ 被恢复成 $\mathcal{Q}_i$. P_e 根据 $O_{e,j}$ 和 $M_{e,j}$ 对 $\left|Q_{i,j}\right\rangle$ 施加 $Z_{O_{e,j} \oplus M_{e,j}} = T_{O_{e,j} \oplus M_{e,j}} \otimes I_2$ 得到

$$\left|W_{i,j}\right\rangle = Z_{O_{e,j} \oplus M_{e,j}} \left|Q_{i,j}\right\rangle, \tag{10}$$

其中 $Z_k = T_k \otimes I_2$ 为全局移动算子, $k \in \mathbb{Z}$, I_2 为 H_c 的单位矩阵. 这样, P_e 就将 $\mathcal{Q}_i$ 转化为 $\mathcal{W}_i$, 其中 $\mathcal{W}_i = \left(\left|W_{i,1}\right\rangle, \left|W_{i,2}\right\rangle, \ldots, \left|W_{i,n}\right\rangle\right)$. 这里, $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, n$, $e = 1, 2, \ldots, N$, 且 $e \neq i$.

步骤 8. 为了进行窃听检测, P_e 制备足够长的随机处于 $\{\left|0\right\rangle, \left|1\right\rangle, \left|+\right\rangle, \left|-\right\rangle\}$ 的诱骗粒子序列, 并将它随机插入 $\mathcal{W}_i$ 从而形成新量子态序列 $\mathcal{W}_i'$. P_e 将 $\mathcal{W}_i'$ 发送回 P_i. 这里, $i = 1, 2, \ldots, N$, $e = 1, 2, \ldots, N$, 且 $e \neq i$.

步骤 9. P_i 收到 P_e 发送过来的 $\mathcal{W}_i'$ 后与 P_e 一起进行窃听检测: P_e 公布诱骗粒子的位置和制备基; P_i 用相应的测量基测量这些诱骗粒子并将测量结果告知 P_e; P_e 分析错误率是否合理. 如果错误率高得不合理, P_e 将认为存在窃听并终止协议; 否则, 协议将被执行下一步. 这里, $i = 1, 2, \ldots, N$, $e = 1, 2, \ldots, N$, 且 $e \neq i$.

步骤 10. 在 P_i 和 P_e 执行完步骤 9 的窃听检测后, $\mathcal{W}_i'$ 被恢复成 $\mathcal{W}_i$. P_i 对 $\left|W_{i,j}\right\rangle$ 施加 $U_m^{-b_j}$ 得到

$$\begin{aligned} \left|Y_{i,j}\right\rangle &= U_m^{-b_j} \left|W_{i,j}\right\rangle = U_m^{-b_j} Z_{O_{e,j} \oplus M_{e,j}} \left|Q_{i,j}\right\rangle \\ &= U_m^{-b_j} \left(T_{O_{e,j} \oplus M_{e,j}} \otimes I_2\right) U_m^{b_j} \left(\left|p_{i,j}\right\rangle \otimes \left|c_{i,j}\right\rangle\right), \end{aligned} \tag{11}$$

然后对 $\left|Y_{i,j}\right\rangle$ 的游走粒子执行 $\{\left|0\right\rangle, \left|1\right\rangle, \ldots, \left|d-1\right\rangle\}$ 基测量得到 $p_{i,j} \oplus O_{e,j} \oplus M_{e,j}$. 由于知道 $p_{i,j}$, P_i 可从 $p_{i,j} \oplus O_{e,j} \oplus M_{e,j}$ 计算出 $X_{e,j}' = O_{e,j} \oplus M_{e,j}$ 并进一步计算出 $\mathcal{X}_e'$ 的哈希值 $h\left(\mathcal{X}_e'\right)$, 其中

$\mathcal{X}'_e = \left(X'_{e,1}, X'_{e,2}, \ldots, X'_{e,n}\right)$. 如果 $h\left(\mathcal{X}'_e\right) = h\left(\mathcal{X}_e\right)$ 对于所有的 $e = 1, 2, \ldots, N$ 且 $e \neq i$ 都成立, P_i 通过量子安全直接通信[30] 向 P_0 发送 $\mathcal{M}_i$. P_0 计算出 $\mathcal{G}_j = \sum_{r=1}^{N} \left(\oplus M_{r,j}\right)$ 并向所有用户公布, $j = 1, 2, \ldots, n$. 最后, P_i 设定最终密钥为

$$\mathcal{K}_j = \left(O_{i,j} \oplus M_{i,j}\right) \oplus \sum_{e} \left[\oplus \left(O_{e,j} \oplus M_{e,j}\right)\right] \ominus \mathcal{G}_j, \tag{12}$$

其中, $\ominus$ 为模 d 减操作, $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, n$, $e = 1, 2, \ldots, N$, 且 $e \neq i$.

4　正确性分析

命题1　所提出的基于圆上双向量子游走的多方认证 QKA 协议的输出是正确的.

证明　文献 [27] 已经证明存在

$$SS^{-1} = I_{2d}, \tag{13}$$

其中 I_{2d} 是大小为 $2d \times 2d$ 的单位矩阵. 利用与文献 [27] 类似的方法可以很容易证明同样存在

$$S^{-1}S = I_{2d}. \tag{14}$$

因此, 根据式 (1), (4) 和 (14) 可以得到

$$U^{-1}U = \left[\left(I_p \otimes R_c\left(\xi, \theta, \zeta\right)\right)^{-1} S^{-1}\right] \left[S \cdot \left(I_p \otimes R_c\left(\xi, \theta, \zeta\right)\right)\right] = I_{2d}. \tag{15}$$

利用 k 次式 (15) 就可产生

$$\left(U^{-1}\right)^k U^k = I_{2d}. \tag{16}$$

另外, 文献 [27] 也已经证明 Z_k 和 U 满足交换律, 即存在

$$Z_k U = U Z_k. \tag{17}$$

根据式 (16) 和 (17), 式 (11) 可进一步被推导为

$$\begin{aligned}
\left|Y_{i,j}\right\rangle &= U_m^{-b_j} Z_{O_{e,j} \oplus M_{e,j}} U_m^{b_j} \left(\left|p_{i,j}\right\rangle \otimes \left|c_{i,j}\right\rangle\right) \\
&= U_m^{-b_j} U_m^{b_j} \left(T_{O_{e,j} \oplus M_{e,j}} \otimes I_2\right) \left(\left|p_{i,j}\right\rangle \otimes \left|c_{i,j}\right\rangle\right) \\
&= \left(T_{O_{e,j} \oplus M_{e,j}} \otimes I_2\right) \left(\left|p_{i,j}\right\rangle \otimes \left|c_{i,j}\right\rangle\right) \\
&= \left(\left|\sum_{a=0}^{d-1} \left[a + \left(O_{e,j} \oplus M_{e,j}\right)\right] \bmod d\right\rangle \langle a| \otimes I_2\right) \left(\left|p_{i,j}\right\rangle \otimes \left|c_{i,j}\right\rangle\right) \\
&= \left|p_{i,j} \oplus O_{e,j} \oplus M_{e,j}\right\rangle \otimes \left|c_{i,j}\right\rangle .
\end{aligned} \tag{18}$$

当 P_i 在步骤 10 使用 $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ 基去测量 $\left|Y_{i,j}\right\rangle$ 的游走粒子时, 可轻易得到 $p_{i,j} \oplus O_{e,j} \oplus M_{e,j}$. 当 P_i 在步骤 10 从 P_0 收到 $\mathcal{G}_j$ 时, 可轻易计算

$$\begin{aligned}
\mathcal{K}_j =& \left(O_{i,j} \oplus M_{i,j}\right) \oplus \sum_{e} \left[\oplus \left(O_{e,j} \oplus M_{e,j}\right)\right] \ominus \mathcal{G}_j \\
=& \left[O_{i,j} \oplus \sum_{e} \left(\oplus O_{e,j}\right)\right] \oplus \left[M_{i,j} \oplus \sum_{e} \left(\oplus M_{e,j}\right)\right] \ominus \mathcal{G}_j \\
=& \left[O_{i,j} \oplus \sum_{e} \left(\oplus O_{e,j}\right)\right] \oplus \left[M_{i,j} \oplus \sum_{e} \left(\oplus M_{e,j}\right)\right] \ominus \sum_{r=1}^{N} \left(\oplus M_{r,j}\right)
\end{aligned}$$

$$=\sum_{r=1}^{N}(\oplus O_{r,j}), \tag{19}$$

其中, $i=1,2,\ldots,N$, $j=1,2,\ldots,n$, $e=1,2,\ldots,N$, 且 $e\neq i$. 因此, 可得出结论: $P_1,P_2,\ldots,P_N$ 都能协商得到相同的最终密钥. 现在可以得出结论: 所提出的基于圆上双向量子游走的多方认证 QKA 协议的输出是正确的.

5　安全性分析

5.1　信息论安全性

命题2　所提出的基于圆上双向量子游走的多方认证 QKA 协议具有信息论安全性.

证明　在本文协议中, 输入的量子游走态的密度矩阵为

$$\rho_{\text{in}}=\frac{1}{2d}\sum_{p=0}^{d-1}\sum_{c=0}^{1}|p\rangle\langle p|\otimes|c\rangle\langle c|=\frac{1}{2d}\sum_{p=0}^{d-1}|p\rangle\langle p|\otimes(|0\rangle\langle 0|+|1\rangle\langle 1|)=\frac{1}{2d}I_d\otimes I_2=\frac{I_{2d}}{2d}, \tag{20}$$

其中 $d=2^l$. 假设 r 是大于等于 0 的随机整数, 在被施加 U^r 进行加密后, 根据式 (16) 和 (20), ρ_{in} 被转化成 [31]

$$\rho_{\text{out}}=U^r\rho_{\text{in}}\left(U^{-1}\right)^r=U^r\frac{I_{2d}}{2d}\left(U^{-1}\right)^r=\frac{U^r(U^{-1})^r}{2d}=\frac{I_{2d}}{2d}. \tag{21}$$

当 r 是小于 0 的整数时可得出相同的结论. 在被施加 Z_k 后, $\rho'_{\text{in}}=\rho_{\text{out}}$ 会被转化为 [31]

$$\rho'_{\text{out}}=Z_k\rho'_{\text{in}}Z_{-k}=Z_k\rho_{\text{out}}Z_{-k}=Z_k\frac{I_{2d}}{2d}Z_{-k}=(T_k\otimes I_2)\frac{I_{2d}}{2d}(T_{-k}\otimes I_2)=\frac{I_{2d}}{2d}. \tag{22}$$

根据式 (21) 和 (22), 输入态 ρ_{in} 在被先后施加 U^r 和 Z_k 后产生的输出态是一个完全混合态.

文献 [32,33] 证实了量子一次一密的信息论安全性. 根据文献 [32,33], 对于一个 l 量子比特系统, 仅当对于每个输入态 ρ_{input}, 输出态 ρ_{output} 是一个满足式 (23) 的完全混合态时, 协议才具有信息论安全性:

$$\rho_{\text{output}}=\sum_j p_jH_j\rho_{\text{input}}H_j^{\dagger}=\frac{I_{2^l}}{2^l}, \tag{23}$$

其中, ρ_{input} 是任意可能输入态的密度矩阵, H_j 是以概率 p_j 被施加在输入态的用于加密的相应酉操作, $H_j^{\dagger}$ 是 H_j 的厄米共轭, I_{2^l} 是 $2^l\times 2^l$ 的单位矩阵. 当输出态是一个满足式 (23) 的完全混合态时, 协议才具有信息论安全性的原因在于: 首先, 所有输入必须被映射到同一个输出密度矩阵 (因为 ρ_{output} 必须独立于输入); 其次, 既然加密操作具有酉性, 完全混合态必须自我映射, 因此存在 $\rho_{\text{output}}=\frac{I_{2^l}}{2^l}$.

可以很容易发现, 式 (21) 和 (22) 被结合起来后会满足式 (23) , 因此本文协议具有信息论安全性.

5.2　来自 Eve 的外在攻击

5.2.1　扮演攻击

当 P_i 向 P_e 发送 $\mathcal{Q}''_i$ 时, Eve 扮演 P_e 去接收 $\mathcal{Q}''_i$ 并与 P_i 一起执行步骤 5 的窃听检测. P_i 在步骤 6 会告知 $\mathcal{Q}'_i$ 中用于身份认证的诱骗粒子的测量基, 然而, Eve 因对 ID_e 不知情而仍不能确定 $\mathcal{Q}'_i$ 中它们的具体位置. 这样, Eve 只能按照自己猜想随机选择 $\mathcal{Q}'_i$ 中用于身份认证的诱骗粒子, 使用 P_i 告诉的测量基测量它们, 然后再公布测量结果. 可以得出结论: Eve 的假冒攻击毫无疑问地会被 P_i 发现.

5.2.2　其他典型外在攻击

在步骤 4 中, P_i 向其他 $N-1$ 个用户分别传送 $N-1$ 个处于 $\mathcal{Q}_i''$ 的新量子态序列, 采用随机处于 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ 的诱骗粒子来检测 Eve 对传输过程发起的外在攻击, 其中 $i=1,2,\ldots,N$. 在步骤 8 中, P_e 向 P_i 传送 $\mathcal{W}_i'$, 也采用随机处于 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ 的诱骗粒子对 Eve 的攻击进行检测, 其中 $i=1,2,\ldots,N$, $e=1,2,\ldots,N$, 且 $e\neq i$. 这种窃听检测方法是由文献 [34,35] 提出的, 可被视作被文献 [36] 证明具有理论上无条件安全性的 BB84 QKD 协议的窃听检测方法的变形. 不失一般性, 这里以 P_e 在步骤 8 向 P_i 传送 $\mathcal{W}_i'$ 为例对 Eve 发起的其他典型外在攻击进行分析.

(1) 测量 – 重发攻击. 当 P_e 向 P_i 传送 $\mathcal{W}_i'$ 时, Eve 拦截 $\mathcal{W}_i'$ 并随机使用 σ_Z 基或 σ_X 基对其量子态进行测量, 再把测量后的序列传递给 P_i. 由于 Eve 对 $\mathcal{W}_i'$ 中的诱骗粒子采用的测量基和 P_e 制备它们时所使用的制备基不一定一致, 如果 $\mathcal{W}_i'$ 中共有 λ 个诱骗粒子, 那么 Eve 对 $\mathcal{W}_i'$ 发起的测量 – 重发攻击被 P_e 和 P_i 检测到的概率为 $1-\left(\frac{3}{4}\right)^{\lambda}$. 显然, 如果 $\lambda\to\infty$, Eve 的这种攻击被检测到的概率将为 1. 这里, σ_Z 基为 $\{|0\rangle, |1\rangle\}$, σ_X 基为 $\{|+\rangle, |-\rangle\}$, $i=1,2,\ldots,N$, $e=1,2,\ldots,N$, 且 $e\neq i$.

(2) 拦截 – 重发攻击. 当 P_e 向 P_i 传送 $\mathcal{W}_i'$ 时, Eve 拦截 $\mathcal{W}_i'$ 并保留在自己手中, 再将随机处于 σ_Z 基或 σ_X 基的假粒子传送给 P_i. 由于 P_e 对诱骗粒子的制备态和 P_i 对 Eve 的假粒子的测量结果不一定对应相同, 如果 $\mathcal{W}_i'$ 中共有 λ 个诱骗粒子, 那么 Eve 对 $\mathcal{W}_i'$ 发起的拦截 – 重发攻击被 P_e 和 P_i 检测到的概率为 $1-\left(\frac{1}{2}\right)^{\lambda}$. 显然, 如果 $\lambda\to\infty$, Eve 的这种攻击被检测到的概率将为 1. 这里, $i=1,2,\ldots,N$, $e=1,2,\ldots,N$, 且 $e\neq i$.

(3) 纠缠 – 测量攻击.

命题3　当 P_e 向 P_i 传送 $\mathcal{W}_i'$ 时, 为了尝试得到有用信息, Eve 对其辅助粒子 $|\rho\rangle$ 与 $\mathcal{W}_i'$ 的粒子一起施加酉操作 U_ξ. 为了使 Eve 的纠缠 – 测量攻击不引入任何错误, Eve 的辅助粒子的最终状态应与 $\mathcal{W}_i'$ 的粒子无关, 从而导致 Eve 无法得到任何有用信息.

证明　当 P_e 向 P_i 传送 $\mathcal{W}_i'$ 时, Eve 对其辅助粒子 $|\rho\rangle$ 与 $\mathcal{W}_i'$ 的粒子一起施加酉操作 U_ξ, 其中 U_ξ 具有如下作用:

$$U_\xi|0\rangle|\rho\rangle=\alpha|0\rangle|\rho_{00}\rangle+\beta|1\rangle|\rho_{01}\rangle, \tag{24}$$

$$U_\xi|1\rangle|\rho\rangle=\gamma|0\rangle|\rho_{10}\rangle+\delta|1\rangle|\rho_{11}\rangle, \tag{25}$$

其中, $|\rho_{00}\rangle$, $|\rho_{01}\rangle$, $|\rho_{10}\rangle$ 和 $|\rho_{11}\rangle$ 为 Eve 的探测态, $|\alpha|^2+|\beta|^2=1$ 和 $|\gamma|^2+|\delta|^2=1$. 由式 (24) 和 (25) 容易得到

$$\begin{aligned}
U_\xi|+\rangle|\rho\rangle&=U_\xi\left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|\rho\rangle\right]\\
&=\frac{1}{\sqrt{2}}\left[(\alpha|0\rangle|\rho_{00}\rangle+\beta|1\rangle|\rho_{01}\rangle)+(\gamma|0\rangle|\rho_{10}\rangle+\delta|1\rangle|\rho_{11}\rangle)\right]\\
&=\frac{1}{\sqrt{2}}\left[|0\rangle(\alpha|\rho_{00}\rangle+\gamma|\rho_{10}\rangle)+|1\rangle(\beta|\rho_{01}\rangle+\delta|\rho_{11}\rangle)\right]\\
&=\frac{1}{2}\left[(|+\rangle+|-\rangle)(\alpha|\rho_{00}\rangle+\gamma|\rho_{10}\rangle)+(|+\rangle-|-\rangle)(\beta|\rho_{01}\rangle+\delta|\rho_{11}\rangle)\right]\\
&=\frac{1}{2}\left[|+\rangle(\alpha|\rho_{00}\rangle+\gamma|\rho_{10}\rangle+\beta|\rho_{01}\rangle+\delta|\rho_{11}\rangle)+|-\rangle(\alpha|\rho_{00}\rangle+\gamma|\rho_{10}\rangle-\beta|\rho_{01}\rangle-\delta|\rho_{11}\rangle)\right],
\end{aligned} \tag{26}$$

$$\begin{aligned}
U_\xi|-\rangle|\rho\rangle&=U_\xi\left[\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)|\rho\rangle\right]\\
&=\frac{1}{\sqrt{2}}\left[(\alpha|0\rangle|\rho_{00}\rangle+\beta|1\rangle|\rho_{01}\rangle)-(\gamma|0\rangle|\rho_{10}\rangle+\delta|1\rangle|\rho_{11}\rangle)\right]\\
&=\frac{1}{\sqrt{2}}\left[|0\rangle(\alpha|\rho_{00}\rangle-\gamma|\rho_{10}\rangle)+|1\rangle(\beta|\rho_{01}\rangle-\delta|\rho_{11}\rangle)\right]
\end{aligned}$$

$$= \frac{1}{2}\left[(|+\rangle + |-\rangle)(\alpha|\rho_{00}\rangle - \gamma|\rho_{10}\rangle) + (|+\rangle - |-\rangle)(\beta|\rho_{01}\rangle - \delta|\rho_{11}\rangle)\right]$$
$$= \frac{1}{2}\left[|+\rangle(\alpha|\rho_{00}\rangle - \gamma|\rho_{10}\rangle + \beta|\rho_{01}\rangle - \delta|\rho_{11}\rangle) + |-\rangle(\alpha|\rho_{00}\rangle - \gamma|\rho_{10}\rangle - \beta|\rho_{01}\rangle + \delta|\rho_{11}\rangle)\right]. \quad (27)$$

为了使 Eve 的攻击不引入任何错误, 由式 (24)∼(27) 可推导出

$$\beta = \gamma = 0, \quad (28)$$
$$\alpha|\rho_{00}\rangle + \gamma|\rho_{10}\rangle - \beta|\rho_{01}\rangle - \delta|\rho_{11}\rangle = 0, \quad (29)$$
$$\alpha|\rho_{00}\rangle - \gamma|\rho_{10}\rangle + \beta|\rho_{01}\rangle - \delta|\rho_{11}\rangle = 0. \quad (30)$$

由式 (28)∼(30) 可进一步推导出

$$\alpha|\rho_{00}\rangle = \delta|\rho_{11}\rangle = |\xi\rangle. \quad (31)$$

将式 (28) 和 (31) 都代入式 (24)∼(27) 可产生

$$U_\xi|0\rangle|\rho\rangle = |0\rangle|\xi\rangle, \quad (32)$$
$$U_\xi|1\rangle|\rho\rangle = |1\rangle|\xi\rangle, \quad (33)$$
$$U_\xi|+\rangle|\rho\rangle = |+\rangle|\xi\rangle, \quad (34)$$
$$U_\xi|-\rangle|\rho\rangle = |-\rangle|\xi\rangle. \quad (35)$$

可以得出结论: 为了使 Eve 的纠缠 – 测量攻击不引入任何错误, Eve 的辅助粒子的最终状态应与 $\mathcal{W}_i'$ 的粒子无关, 从而导致 Eve 无法得到任何有用信息.

5.3　内部攻击

Gao 等 [37] 于 2007 年指出, 内部不忠诚用户的攻击通常比外部窃听者的攻击带来更大的危害. 接下来详细分析本文协议针对内部用户攻击的安全性.

5.3.1　来自半忠诚第三方 P_0 的攻击

在本文协议中, P_0 被认为是半忠诚的, 因此不能与 P_i 合谋, 其中 $i = 1, 2, \ldots, N$. 为了获取用户的私钥 $\mathcal{O}_i$ 或最终密钥 $\mathcal{K}_j$, P_0 可能会对 P_i 在步骤 4 向其他 $N-1$ 个用户分别传送的 $N-1$ 个处于 $\mathcal{Q}_i''$ 的新量子态序列或 P_e 在步骤 8 向 P_i 传送的 $\mathcal{W}_i'$ 发起攻击, 其中 $i = 1, 2, \ldots, N$, $e = 1, 2, \ldots, N$, 且 $e \neq i$. 然而, 由于这时 P_0 本质上是一个外部攻击者, 根据 5.2 小节的分析, 其攻击会不可避免地被检测到.

退一步讲, 即使 P_0 可以知道 $p_{i,j} \oplus O_{e,j} \oplus M_{e,j}$, 但由于对 $p_{i,j}$ 一无所知, P_0 仍不能得到 $X'_{e,j} = O_{e,j} \oplus M_{e,j}$. P_0 通过量子安全直接通信从 P_i 收到 $\mathcal{M}_i$, 但仍无法得到 $O_{e,j}$. 虽然 P_0 可计算出 $\mathcal{G}_j = \sum_{r=1}^{N}(\oplus M_{r,j})$, 但仍不能通过计算式 (12) 得到最终密钥 $\mathcal{K}_j$. 这里, $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, n$, $e = 1, 2, \ldots, N$, 且 $e \neq i$.

5.3.2　来自单个不忠诚用户的攻击

当单个不忠诚用户对其他任意两个用户之间的量子态传输进行攻击时, 由于他这时本质上属于一个外在攻击者, 根据 5.2 小节的分析, 其攻击会毫无疑问地被发现.

单个不忠诚用户 P_i 对 $|Y_{i,j}\rangle$ 的游走粒子执行 $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ 基测量得到 $p_{i,j} \oplus O_{e,j} \oplus M_{e,j}$, 并可进一步根据 $p_{i,j}$ 和 $p_{i,j} \oplus O_{e,j} \oplus M_{e,j}$ 计算出 $X'_{e,j} = O_{e,j} \oplus M_{e,j}$. 这里, i 为 $\{1, 2, \ldots, N\}$ 中的某个数, $j = 1, 2, \ldots, n$, $e = 1, 2, \ldots, N$, 且 $e \neq i$. 但由于不知道 $M_{e,j}$, P_i 仍无法得到 $O_{e,j}$. 退一步讲, 如

果单个不忠诚用户 P_i 知道 $O_{e,j}$ 就会试图发起以下欺骗攻击来随心所欲地将最终的共享密钥设置为 $\mathcal{K}_j^*$: P_i 对 $|Q_{e,j}\rangle$ 施加 $T_{F_{i,j}}\otimes I_2$ 得到

$$\left|W_{e,j}^*\right\rangle=\left(T_{F_{i,j}}\otimes I_2\right)|Q_{e,j}\rangle\,, \tag{36}$$

其中 $F_{i,j}=\mathcal{K}_j^*\oplus M_{i,j}\ominus\sum_e(\oplus O_{e,j})$; P_i 将 $|W_{e,j}^*\rangle$ 发送给 P_e; P_e 对 $|W_{e,j}^*\rangle$ 的游走粒子进行 $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$ 基测量得到 $p_{e,j}\oplus F_{i,j}$, 并进一步根据 $p_{e,j}$ 和 $p_{e,j}\oplus F_{i,j}$ 计算出 $F_{i,j}$; 若 P_0 向所有用户公布 $\mathcal{G}_j$, P_e 计算

$$\mathcal{K}_j^*=(O_{e,j}\oplus M_{e,j})\oplus\sum_{r\neq e,r\neq i}[\oplus(O_{r,j}\oplus M_{r,j})]\oplus\mathcal{K}_j^*\oplus M_{i,j}\ominus\sum_e(\oplus O_{e,j})\ominus\mathcal{G}_j \tag{37}$$

只能得到最终共享密钥为 $\mathcal{K}_j^*$. 幸运的是, P_i 因无法知道 $O_{e,j}$ 从而不能发起上述攻击; 而且, 由于 $h(\mathcal{F}_i)\neq h(\mathcal{X}_i)$, P_e 就不会通过量子安全直接通信向 P_0 发送 $\mathcal{M}_e$, 其中 $\mathcal{F}_i=(F_{i,1},F_{i,2},\ldots,F_{i,n})$.

5.3.3　来自多个不忠诚用户的共谋攻击

(1) 首先分析合谋人数为 $N-2$ 这种情况. 不失一般性, 假设忠诚用户只有 P_a 和 P_b, 其中 a 和 b 为 $\{1,2,\ldots,N\}$ 中的两个数.

当 $N-2$ 个不忠诚用户联合起来对 P_a 和 P_b 之间的量子态传输进行攻击时, 由于 $N-2$ 个不忠诚用户这时本质上属于外在攻击者, 根据 5.2 小节的分析, 其攻击会毫无疑问地被发现.

$N-2$ 个不忠诚用户很容易得到 $X'_{a,j}=O_{a,j}\oplus M_{a,j}$ 和 $X'_{b,j}=O_{b,j}\oplus M_{b,j}$, 其中 $j=1,2,\ldots,n$. 但由于不知道 $M_{a,j}$ 和 $M_{b,j}$, 他们仍无法得到 $O_{a,j}$ 和 $O_{b,j}$. 退一步讲, 如果他们知道 $O_{a,j}$ 和 $O_{b,j}$ 就会试图发起以下欺骗攻击来随心所欲地将最终的共享密钥设置为 $\mathcal{K}_j^{\#}$ (为描述方便, 以下将 $N-2$ 个不忠诚用户看成一个整体): 他们对 $|Q_{a,j}\rangle$ 施加 $T_{F_{f_a,j}}\otimes I_2$ 得到

$$\left|W_{a,j}^{\#}\right\rangle=\left(T_{F_{f_a,j}}\otimes I_2\right)|Q_{a,j}\rangle\,, \tag{38}$$

其中 $F_{f_a,j}=\mathcal{K}_j^{\#}\oplus\sum_{r\neq a,r\neq b}M_{r,j}\ominus(O_{a,j}\oplus O_{b,j})$; 他们对 $|Q_{b,j}\rangle$ 施加 $T_{F_{f_b,j}}\otimes I_2$ 得到

$$\left|W_{b,j}^{\#}\right\rangle=\left(T_{F_{f_b,j}}\otimes I_2\right)|Q_{b,j}\rangle\,, \tag{39}$$

其中 $F_{f_b,j}=F_{f_a,j}$; 他们将 $|W_{a,j}^{\#}\rangle$ 和 $|W_{b,j}^{\#}\rangle$ 分别发送给 P_a 和 P_b; P_a 对 $|W_{a,j}^{\#}\rangle$ 的游走粒子进行 $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$ 基测量得到 $p_{a,j}\oplus F_{f_a,j}$, 并进一步根据 $p_{a,j}$ 和 $p_{a,j}\oplus F_{f_a,j}$ 计算出 $F_{f_a,j}$; P_b 对 $|W_{b,j}^{\#}\rangle$ 的游走粒子进行 $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$ 基测量得到 $p_{b,j}\oplus F_{f_b,j}$, 并进一步根据 $p_{b,j}$ 和 $p_{b,j}\oplus F_{f_b,j}$ 计算出 $F_{f_b,j}$; 若 P_0 向所有用户公布 $\mathcal{G}_j$, P_a 和 P_b 计算

$$\mathcal{K}_j^{\#}=(O_{a,j}\oplus M_{a,j})\oplus(O_{b,j}\oplus M_{b,j})\oplus\mathcal{K}_j^{\#}\oplus\sum_{r\neq a,r\neq b}M_{r,j}\ominus(O_{a,j}\oplus O_{b,j})\ominus\mathcal{G}_j \tag{40}$$

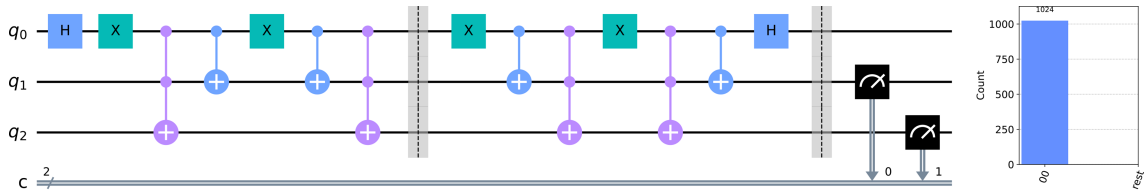
只能得到最终共享密钥为 $\mathcal{K}_j^{\#}$. 幸运的是, $N-2$ 个不忠诚用户因无法知道 $O_{a,j}$ 和 $O_{b,j}$ 从而不能发起上述攻击; 而且, 由于步骤 10 的哈希认证不能全通过, P_a 和 P_b 不会通过量子安全直接通信分别向 P_0 发送 $\mathcal{M}_a$ 和 $\mathcal{M}_b$.

综上所述, 本文协议可抵抗 $N-2$ 个不忠诚用户的共谋攻击.

(2) 接着分析合谋人数为 $N-1$ 这种最坏的情况. 假设忠诚用户只有 P_c, 其中 c 为 $\{1,2,\ldots,N\}$ 中的某个数.

$N-1$ 个不忠诚用户很容易得到 $X'_{c,j}=O_{c,j}\oplus M_{c,j}$, 其中 $j=1,2,\ldots,n$. 但由于不知道 $M_{c,j}$, 他们仍无法得到 $O_{c,j}$. 退一步讲, 如果他们知道 $O_{c,j}$ 就会试图发起以下欺骗攻击来随心所欲地将最终的共享密钥设置为 $\mathcal{K}_j^{@}$ (为描述方便, 以下将 $N-1$ 个不忠诚用户看成一个整体): 他们对 $|Q_{c,j}\rangle$ 施加 $T_{F_{f_c,j}}\otimes I_2$ 得到

$$\left|W_{c,j}^{@}\right\rangle=\left(T_{F_{f_c,j}}\otimes I_2\right)|Q_{c,j}\rangle\,, \tag{41}$$



(a)　(b)

图 1　(网络版彩图) (a) $U^{-1}U|0\rangle\otimes|0\rangle$ 的量子线路仿真; (b) 图 (a) 的仿真结果.

Figure 1　(Color online) (a) Quantum circuit simulation of $U^{-1}U|0\rangle\otimes|0\rangle$; (b) simulation results of (a).

其中 $F_{f_c,j}=\mathcal{K}_j^{@}\oplus\sum_{r\neq c}M_{r,j}\ominus O_{c,j}$; 他们将 $|W_{c,j}^{@}\rangle$ 发送给 P_c; P_c 对 $|W_{c,j}^{@}\rangle$ 的游走粒子进行 $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$ 基测量得到 $p_{c,j}\oplus F_{f_c,j}$, 并进一步根据 $p_{c,j}$ 和 $p_{c,j}\oplus F_{f_c,j}$ 计算出 $F_{f_c,j}$; 若 P_0 向所有用户公布 $\mathcal{G}_j$, P_c 计算

$$\mathcal{K}_j^{@}=(O_{c,j}\oplus M_{c,j})\oplus\mathcal{K}_j^{@}\oplus\sum_{r\neq c}M_{r,j}\ominus O_{c,j}\ominus\mathcal{G}_j \tag{42}$$

只能得到最终共享密钥为 $\mathcal{K}_j^{@}$. 幸运的是, $N-1$ 个不忠诚用户因无法知道 $O_{c,j}$ 从而不能发起上述攻击; 而且, 由于步骤 10 的哈希认证不能全通过, P_c 不会通过量子安全直接通信分别向 P_0 发送 $\mathcal{M}_c$.

综上所述, 本文协议可抵抗 $N-1$ 个不忠诚用户的共谋攻击.

6　基于 IBM Qiskit 的量子线路仿真

在忽略窃听检测过程和身份认证过程后, 这部分利用 IBM 的 Qiskit 对本文协议进行量子线路仿真以验证其输出正确性. 以下所有仿真实验都进行 1024 次, 且量子游走系统中 $R_c\,(0,\theta_m,0)$ 都为哈达玛 (Hadamard) 门.

不失一般性, 假设 $d=2^l=4$, 则量子游走态由 $l+1=3$ 个量子比特 $q_2q_1q_0$ 构成, 其中 q_2q_1 表示游走粒子, q_0 表示硬币粒子. U 和 U^{-1} 的量子线路可根据文献 [38] 得到. $U^{-1}U\,|0\rangle\otimes|0\rangle$ 的量子线路仿真如图 1(a) 所示, 其中输入默认为 $|0\rangle\otimes|0\rangle$, 第一条虚线左侧表示施加一次 U, 第二条虚线左侧表示施加一次 U^{-1}, 第二条虚线右边表示对最终的游走粒子执行 $\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}$ 基测量; 测量结果如图 1(b) 所示, 其中横坐标中 "00" 指代测量结果为 $|0\rangle$, 横坐标中 "rest" 指代测量结果为 $|1\rangle$, $|2\rangle$ 和 $|3\rangle$, 纵坐标中 "Count" 指代得到相应测量结果的仿真实验发生的次数. 根据图 1(b) 可知, 1024 次仿真实验对游走粒子的 $\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}$ 基测量结果均为 $|0\rangle$, 从而验证了 U 的幺正性, 即存在 $U^{-1}U=I_{2d}$. 同样地, 不难验证 $(U^{-1})^kU^k=I_{2d}$. 对量子游走态施加 U^k 会使得游走粒子的状态出现随机性, 从而起到加密作用.

T_k 的量子线路也可根据文献 [38] 得到. 由于 $Z_k=T_k\otimes I_2=T_k\,|0\rangle\langle 0|+T_k\,|1\rangle\langle 1|$, Z_k 的量子线路由依次受 $|0\rangle$ 和 $|1\rangle$ 控制的 T_k 构成 [39], 其中 X 门用于触发 $|0\rangle$ 控制, 再由另一个 X 门将其翻转回 $|1\rangle$ 控制. $Z_{-1}Z_1\,|0\rangle\otimes|0\rangle$ 的量子线路仿真如图 2(a) 所示, 其中输入默认为 $|0\rangle\otimes|0\rangle$, 第一条虚线左侧表示施加 Z_1, 第二条虚线左侧表示施加 Z_{-1}, 第二条虚线右侧表示对最终的游走粒子执行 $\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}$ 基测量; 测量结果如图 2(b) 所示, 其中横坐标中 "00" 指代测量结果为 $|0\rangle$, 横坐标中 "rest" 指代测量结果为 $|1\rangle$, $|2\rangle$ 和 $|3\rangle$, 纵坐标中 "Count" 指代得到相应测量结果的仿真实验发生的次数. 根据图 2(b) 可知, 1024 次仿真实验对游走粒子的 $\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}$ 基测量结果均为 $|0\rangle$, 从而验证了 Z_1 的幺正性, 即存在 $Z_{-1}Z_1=I_{2d}$. 同样地, 不难验证 $Z_{-k}Z_k=I_{2d}$.

$U^{-4}Z_3U^4\,|3\rangle\otimes|0\rangle$ 的量子线路仿真如图 3(a) 所示, 其中第一条虚线左侧表示输入为 $|3\rangle\otimes|0\rangle$, 第二条虚线左侧依次表示施加封装后的 U^4, Z_3 和 U^{-4}, 第二条虚线右侧表示对最终的游走粒子执行 $\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}$ 基测量; 测量结果如图 3(b) 所示, 其中横坐标中 "10" 指代测量结果为 $|2\rangle$, 横坐标中 "rest" 指代测量结果为 $|0\rangle$, $|1\rangle$ 和 $|3\rangle$, 纵坐标中 "Count" 指代得到相应测量结果的仿真实验发生的

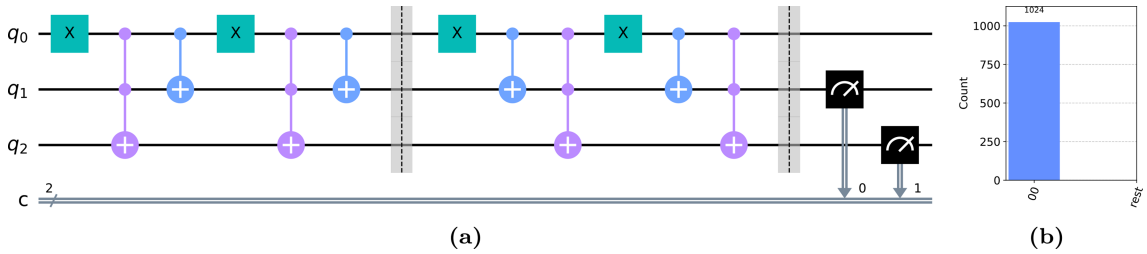


图 2　(网络版彩图) (a) $Z_{-1}Z_1\left|0\right\rangle\otimes\left|0\right\rangle$ 的量子线路仿真; (b) 图 (a) 的仿真结果.

Figure 2　(Color online) (a) Quantum circuit simulation of $Z_{-1}Z_1\left|0\right\rangle\otimes\left|0\right\rangle$; (b) simulation results of (a).

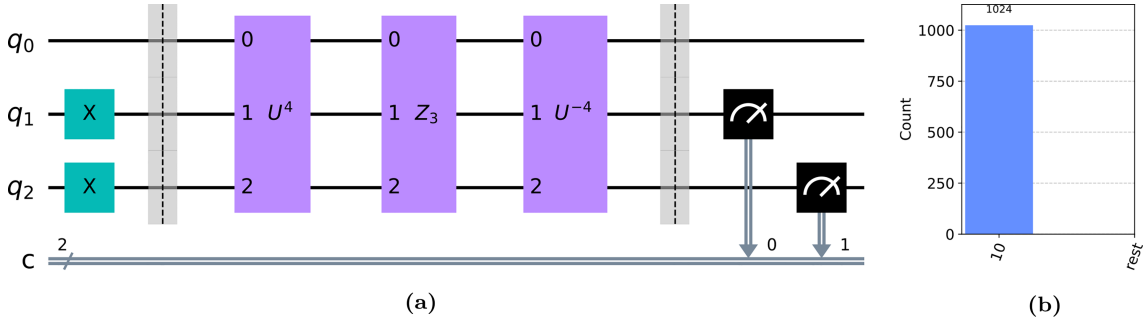


图 3　(网络版彩图) (a) $U^{-4}Z_3U^4\left|3\right\rangle\otimes\left|0\right\rangle$ 的量子线路仿真; (b) 图 (a) 的仿真结果.

Figure 3　(Color online) (a) Quantum circuit simulation of $U^{-4}Z_3U^4\left|3\right\rangle\otimes\left|0\right\rangle$; (b) simulation results of (a).

次数. 根据图 3(b) 可知, 1024 次仿真实验对游走粒子的 $\{\left|0\right\rangle,\left|1\right\rangle,\left|2\right\rangle,\left|3\right\rangle\}$ 基测量结果均为 $\left|2\right\rangle$, 从而验证了 Z_k 和 U 的交换律, 即存在 $Z_kU=UZ_k$, 从而进一步得到 $U^{-4}Z_3U^4\left|3\right\rangle\otimes\left|0\right\rangle=Z_3\left|3\right\rangle\otimes\left|0\right\rangle=\left|(3+3)\bmod 4\right\rangle\otimes\left|0\right\rangle=\left|2\right\rangle\otimes\left|0\right\rangle$.

7　讨论

QKA 协议的量子比特效率通常被定义为 [40]

$$\kappa=\frac{\tau_s}{\tau_q+\tau_c},\tag{43}$$

其中 τ_s 表示用户们最终共享的密钥比特数, τ_q 表示协议花掉的量子比特数, τ_c 表示协议花掉的经典比特数. 本文在计算量子比特效率时忽略窃听检测所花掉的所有量子和经典资源.

在本文协议中, P_i 在步骤 10 设定最终密钥为式 (12) 的 $\mathcal{K}_j$, 其中 $i=1,2,\ldots,N$, $j=1,2,\ldots,n$, 因此有 $\tau_s=nl$ 比特. P_i 在步骤 2 制备 $N-1$ 个处于 $\mathcal{Q}_i$ 的量子态序列, P_i 在步骤 3 生成 $N-1$ 个长度均为 n 的随机处于 $\{\left|0\right\rangle,\left|1\right\rangle,\left|+\right\rangle,\left|-\right\rangle\}$ 的诱骗粒子序列用于身份认证, P_i 通过量子安全直接通信 [30] 向 P_0 发送 $\mathcal{M}_i$, 其中 $i=1,2,\ldots,N$, 因此有 $\tau_q=N(N-1)(l+1)n+N(N-1)n+Nln=Nn[N(l+2)-2]$ 量子比特. P_i 在步骤 1 向其他用户公布 $h(\mathcal{X}_i)$; P_i 在步骤 6 告知 P_e $\mathcal{Q}_i'$ 中用于身份认证的诱骗粒子的测量基但不告诉它们的具体位置, P_e 根据 ID_e 将相应位置的用于身份认证的诱骗粒子提取出来并使用 P_i 告知的测量基对它们进行测量, 然后将测量结果告知 P_i; P_0 在步骤 10 并向所有用户公布 $\mathcal{G}_j$; 这里, $i=1,2,\ldots,N$, $e=1,2,\ldots,N$, 且 $e\neq i$, $j=1,2,\ldots,n$; 因此有 $\tau_c=NY+N(N-1)(n+n)+nl=NY+2N(N-1)n+nl$, 其中 Y 是 $h(\cdot)$ 的输出比特数. 可以得出结论, 本文协议的量子比特效率为 $\kappa=\frac{nl}{Nn[N(l+2)-2]+NY+2N(N-1)n+nl}$.

接下来将本文协议和文献 [18~26] 的身份认证 QKA 协议进行对比, 对比结果被总结在表 1 中. 根据表 1, 本文协议在量子资源上胜过文献 [18~21, 23~26] 的协议, 这是因为本文协议采用更容易被

表 1　本文协议和之前的身份认证 QKA 协议之间的对比.

Table 1　Comparison between the proposed protocol and previous authentication QKA protocols.

	Quantum resource	Identity authentications	Number of users	Quantum measurement	Usage of Hash	Usage of unitary operations	Usage of quantum entanglement swapping
Ref. [18]	GHZ-like states	Yes	2	Single-particle measurements	Yes	Yes	No
Ref. [19]	Single-particle states and Bell states	Yes	3 or N	Single-particle measurements and GHZ basis measurements	Yes	Yes	Yes
Ref. [20]	Single-particle states and Bell states	Yes	2	Single-particle measurements and Bell basis measurements	Yes	No	Yes
Ref. [21]	GHZ states	Yes	3	Single-particle measurements	No	Yes	No
Ref. [22]	Two-particle product states	Yes	N	Single-particle measurements	Yes	Yes	No
Ref. [23]	Single-particle states and GHZ states	Yes	N	Single-particle measurements and Bell basis measurements	No	No	Yes
Ref. [24]	Single-particle states and six-particle entangled states	Yes	2	Single-particle measurements and Bell basis measurements	No	Yes	Yes
Ref. [25]	Single-particle states and Bell states	Yes	2	Single-particle measurements and Bell basis measurements	Yes	Yes	No
Ref. [26]	Single-particle states and four-particle cluster states	Yes	N	Single-particle measurements and four-particle cluster measurements	Yes	Yes	Yes
This protocol	Single-particle states and two-particle product states	Yes	N	Single-particle measurements	Yes	Yes	No

制备的两粒子乘积态作为初始量子资源而非量子纠缠态; 在量子测量方面, 本文协议仅使用单粒子测量, 优于文献 [19,20,23∼26] 的协议; 在量子纠缠交换的使用上, 本文协议优于文献 [19,20,23,24,26] 的协议.

8　总结

在 QKA 的实际应用中, 如何验证用户身份的真实性是一个关键问题, 但之前的许多 QKA 协议忽略了这一问题, 从而对假冒攻击未必是安全的. 本文将 QIA 应用到多方 QKA 中提出一种新颖的基于圆上双向量子游走的多方认证 QKA 协议, 使得 N 个用户经过相互身份认证后在一个半忠诚第三方的协助下能平等地协商出最终的共享密钥, 具有更强的身份认证可靠性. 理论上的输出正确性分析和 IBM Qiskit 量子云平台上进行的量子线路仿真都证实了该协议的输出正确性. 该协议仅采用两粒子乘积态而非量子纠缠态作为初始量子资源, 且仅需要酉操作和单粒子测量. 该协议被证实具备信息论安全性, 能抵抗 Eve 发起的外在攻击, 且能抵抗 $N-1$ 个不忠诚用户发起的共谋攻击.

参考文献

1　Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the International Conference on Computers, Systems and Signal Processing, 1984. 175–179

2　Zhou N, Zeng G, Xiong J. Quantum key agreement protocol. Electron Lett, 2004, 40: 1149–1150

3　Hsueh C, Chen C. Quantum key agreement protocol with maximally entangled states. In: Proceedings of the 14th Information Security Conference, 2004. 236–242

4　Tsai C, Hwang T. On "quantum key agreement protocol". Technical Report, CSIE, NCKU, 2009

5　Shi R H, Zhong H. Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf Process, 2013, 12: 921–932

6　Liu B, Gao F, Huang W, et al. Multiparty quantum key agreement with single particles. Quantum Inf Process, 2013, 12: 1797–1805

7　Sun Z, Zhang C, Wang B, et al. Improvements on "multiparty quantum key agreement with single particles". Quantum Inf Process, 2013, 12: 3411–3420

8　Xu G B, Wen Q Y, Gao F, et al. Novel multiparty quantum key agreement protocol with GHZ states. Quantum Inf Process, 2014, 13: 2587–2594

9　Sun Z, Yu J, Wang P. Efficient multi-party quantum key agreement by cluster states. Quantum Inf Process, 2016, 15: 373–384

10 Gu J, Hwang T. Improvement of “novel multiparty quantum key agreement protocol with GHZ states”. Int J Theor Phys, 2017, 56: 3108–3116

11 Yin X R, Ma W P. Multiparty quantum key agreement based on three-photon entanglement with unidirectional qubit transmission. Int J Theor Phys, 2019, 58: 631–638

12 Liu H N, Liang X Q, Jiang D H, et al. Multi-party quantum key agreement protocol with Bell states and single particles. Int J Theor Phys, 2019, 58: 1659–1666

13 Tang R H, Zhang C, Long D Y, et al. Improvements on “multi-party quantum key agreement protocol with bell states and single particles”. Int J Theor Phys, 2020, 59: 1623–1637

14 Tang J, Shi L, Wei J, et al. Novel multi-party quantum key agreement protocols under collective noise. Mod Phys Lett B, 2021, 35: 2150137

15 Gao H, Zhou R G. Multi-party quantum key agreement protocol based on G-like states and χ + states. Int J Theor Phys, 2022, 61: 16

16 Yang H, Lu S, Zhou Q, et al. Efficient single-state multi-party quantum key agreement. Quantum Inf Process, 2024, 23: 150

17 Crépeau C, Salvail L. Quantum oblivious mutual identification. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, 1995. 133–146

18 Zhu H, Wang C, Li Z. Semi-honest three-party mutual authentication quantum key agreement protocol based on GHZ-like state. Int J Theor Phys, 2021, 60: 293–303

19 Wu Y T, Chang H, Guo G D, et al. Multi-party quantum key agreement protocol with authentication. Int J Theor Phys, 2021, 60: 4066–4077

20 He Y F, Pang Y, Di M. Mutual authentication quantum key agreement protocol based on Bell states. Quantum Inf Process, 2022, 21: 290

21 Xu Y, Wang C, Cheng K, et al. A novel three-party mutual authentication quantum key agreement protocol with GHZ states. Int J Theor Phys, 2022, 61: 245

22 Gao L Z, Zhang X, Lin S, et al. Authenticated multiparty quantum key agreement for optical-ring quantum communication networks. Front Phys, 2022, 10: 962781

23 Li G D, Cheng W C, Wang Q L, et al. A measurement device independent multi-party quantum key agreement protocol with identity authentication. Quantum Inf Process, 2023, 22: 443

24 Guo J H, Bai M Q, Lei X Y, et al. Improved quantum key agreement protocol with authentication. Chin Phys B, 2023, 32: 050310

25 Wang C, Zhang Q, Liang S, et al. Secure mutual authentication quantum key agreement scheme for two-party setting with key recycling. Quantum Inf Process, 2024, 23: 139

26 Zhang L, Han Z, Li Y, et al. Authenticated multi-party quantum key agreement protocol based on cluster states. Laser Phys, 2024, 34: 095205

27 Chen F L, Zhang H, Chen S G, et al. Novel two-party quantum private comparison via quantum walks on circle. Quantum Inf Process, 2021, 20: 178

28 Wang J T, Lian J Y, Ye T Y. Multi-party quantum private comparison of size relationship based on one-direction quantum walks on a circle. Sci China Inf Sci, 2025, 68: 129502

29 Wang J-T, Li X, Ye T-Y. A quantum secure multi-party summation protocol based on one-direction quantum walks on a circle. Sci Sin-Phys Mech Astron, 2024, 54: 240311 [王锦涛, 李霞, 叶天语. 基于圆上单向量子游走的量子安全多方求和协议. 中国科学: 物理学 力学 天文学, 2024, 54: 240311]

30 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319

31 Vlachou C, Rodrigues J, Mateus P, et al. Quantum walk public-key cryptographic system. Int J Quantum Inform, 2015, 13: 1550050

32 Ambainis A, Mosca M, Tapp A, et al. Private quantum channels. In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science, 2000. 547–553

33 Boykin P O, Roychowdhury V. Optimal encryption of quantum bits. Phys Rev A, 2003, 67: 042317

34 Li C-Y, Zhou H-Y, Wang Y, et al. Secure quantum key distribution network with Bell states and local unitary operations. Chin Phys Lett, 2005, 22: 1049–1052

35 Li C-Y, Li X-H, Deng F-G, et al. Efficient quantum cryptography network without entanglement and quantum memory. Chin Phys Lett, 2006, 23: 2896–2899

36 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444

37 Gao F, Qin S, Wen Q, et al. A simple participant attack on the Bradler-Dusek protocol. Quantum Inf Comput,

2007, 7: 329–334
38 Douglas B L, Wang J B. Efficient quantum circuit implementation of quantum walks. Phys Rev A, 2009, 79: 052335
39 Wang J T, Gan Z G, Ye T Y. Quantum scalar product via quantum walks. Phys Lett A, 2025, 536: 130304
40 Cabello A. Quantum key distribution in the Holevo limit. Phys Rev Lett, 2000, 85: 5635–5638

Multiparty quantum key agreement with identity authentication based on two-direction quantum walks on a circle

Zheng WANG, Jintao WANG, Xia LI & Tianyu YE*

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China
* Corresponding author. E-mail: yetianyu@zjgsu.edu.cn

Abstract In this paper, a novel multiparty quantum key agreement with identity authentication based on two-direction quantum walks on a circle, which can accomplish the goal that N users can equally negotiate the final shared key with the help of the semi-honest third party after mutual identity authentications. In this protocol, the users utilize the two-direction evolution operator to encrypt the initial quantum walk states and adopt decoy particles to authenticate the identities of other users; and then, other users employ the global shifting operator to encode their own private keys on the received quantum states. Both the output correctness analysis and the quantum circuit simulations on the IBM Qiskit quantum cloud platform validate the output correctness of this protocol. This protocol only adopts two-particle product states rather than quantum entangled states as the initial quantum resource and only needs unitary operations and single-particle measurements. This protocol is proven to have information-theoretical security, and not only be able to resist the outside attacks from Eve but also be capable of defeating the collusion attacks from $N-1$ dishonest users.

Keywords quantum key agreement, quantum identity authentication, two-direction quantum walks on a circle